WHAT IS CLAIMED IS:

1. A computer program product comprising processor executable instructions for programming a non-volatile storage element in a data processing system, the instructions being stored on a computer readable medium, comprising:

computer code means for encrypting a digital signature using a first encryption key;

computer code means for passing the encrypted signature to a kernel routine;

computer code means, responsive to successfully decrypting the encrypted signature using a second encryption key, for transitioning the data processing system from a protected-mode to a real-mode; and

real-mode computer code means for flash programming the non-volatile storage element.

2. The computer program product of claim 1, wherein the code means for encrypting the digital signature is non-privileged code.

3. The computer program product of claim 2, wherein the code means for passing the encrypted signature to the kernel routine comprises code means for executing a system call from the non-privileged code and passing the signature as a parameter of the system call.

4. The computer program product of claim 1, wherein the first encryption key is a private key and the second encryption key is a public key, wherein the public key and private key are generated from a common algorithm.

5. The computer program product of claim 1, further comprising code means for generating the digital signature, wherein the digital signature includes information that is indicative of the data processing system.

6. The computer program product of claim 5, wherein the digital signature is generated based at least in part upon dynamic information.

7. The computer program product of claim 6, wherein the digital signature is generated at least in part based further upon information including a corresponding hostname and process ID.

8. The computer program product of claim 1, further comprising code means for generating a random number as the digital signature.

9. A data processing system including at least one processor, memory, and input means connected to a common bus, wherein the system memory contains at least a portion of a sequence of computer executable instructions for programming a non-volatile storage element of the data processing system, the instructions comprising:

computer code means for encrypting a digital signature using a first encryption key;

computer code means for passing the encrypted signature to a kernel routine;

computer code means, responsive to successfully decrypting the encrypted signature using a second encryption key, for transitioning the data processing system from a protected-mode to a real-mode; and

real-mode computer code means for flash programming the non-volatile storage element.

10. The data processing system of claim 9, wherein the code means for encrypting the digital signature is non-privileged code.

11. The data processing system of claim 10, wherein the code means for passing the encrypted signature to the kernel routine comprises code means for executing a system call from the non-privileged code and passing the signature as a parameter of the system call.

12. The data processing system of claim 9, wherein the first encryption key is a private key and the second encryption key is a public key, wherein the public key and private key are generated from a common algorithm.

13. The data processing system of claim 9, further comprising code means for generating the digital signature, wherein the digital signature includes information that is indicative of the data processing system.

14. The data processing system of claim 13, wherein the digital signature is generated based at least in part upon dynamic information.

15. The data processing system of claim 14, wherein the digital signature is generated at least in part based further upon information including a corresponding hostname and process ID.

16. The data processing system of claim 9, further comprising code means for generating a random number as the digital signature.

17. A method of programming a non-volatile storage element in a data processing system, comprising:

encrypting a digital signature using a first encryption key;

passing the encrypted signature to a kernel code routine;

responsive to successfully decrypting the encrypted signature using a second encryption key, transitioning the data processing system from a protected-mode to a real-mode with the kernel code routine; and

flash programming the non-volatile storage element in real mode.

18. The method of claim 17, wherein encrypting the digital signature comprises encrypting the digital signature with non-privileged code.

19. The method of claim 18, wherein passing the encrypted signature to the kernel routine comprises executing a system call from the non-privileged code and passing the signature as a parameter of the system call.

20. The method of claim 17, wherein the first encryption key is a private key and the second encryption key is a public key, wherein the public key and private key are generated from a common algorithm.

21. The method of claim 17, further comprising generating the digital signature, wherein the digital signature includes information that is indicative of the data processing system.

22. The method of claim 21, wherein the digital signature is generated based at least in part upon dynamic information.

23. The method of claim 22, wherein the digital signature is generated at least in part based further upon information including a corresponding hostname and process ID.

24. The method of claim 17, further comprising code means for generating a random number as the digital signature.